ABSTRACT OF THE DISCLOSURE:

The objective of this invention is to provide continuous remote authenticated operations for ensuring proper content processing and management in remote untrusted computing environment. The method is based on using a program that was hidden within the content protection program at the remote untrusted computing environment, e.g., an end station. The hidden program can be updated dynamically and it includes an inseparable and interlocked functionality for generating a pseudo random sequence of security signals. Only the media server that sends the content knows how the pseudo-random sequence of security signals were generated; therefore, the media server is able to check the validity of the security signals, and thereby, verify the authenticity of the programs used to process content at the remote untrusted computing environment. If the verification operation fails, the media server will stop the transmission of content to the remote untrusted computing environment.